UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/501,823	12/28/2004	Sebastien Canard	5284-41PUS	6387

27799 7590 04/09/2007

COHEN, PONTANI, LIEBERMAN & PAVANE
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
HOANG, DANIEL L	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/501,823	CANARD ET AL.	
	Examiner	Art Unit	
	Daniel L. Hoang	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *7/19/04* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/19/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-7 are presented.

Allowable Subject Matter

1. Claim 5 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claim 1 recites the limitation "the identifiers stored in the storage means" in line 13. There is insufficient antecedent basis for this limitation in the claim. For purposes of examination, examiner interprets the claim language as follows: "the identifier stored in the storage means." Appropriate correction required.

2. Claim 5 recites the limitation "the counter" in claim 1. There is insufficient antecedent basis for this limitation in the claim. For purposes of examination, examiner is interpreting the claim language as follows: "it verifies that the value of the number of identifiers and the read value are the same." Appropriate correction required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-7 are rejected under 35 U.S.C. 102(b) as being anticipated by Le Roux, US Patent No. 5,191,193.

As per claims 1 and 7, Le Roux teaches:

A cryptographic method implemented by a smart card (30) of a set of smart cards each belonging to a first entity that may be different for each smart card, each smart card being equipped with a chip (31) comprising storage means (32) in which are stored a secret key and an identifier of the first entity that is the proprietor of the smart card (30) and calculation means (33) which execute a cryptographic algorithm whose input arguments include at least the secret key, which method is characterized in that it comprises the following steps:

[see fig. 1, element 1]

before any calculation by the calculation means (33) of the chip (31) of the smart card (30), the chip (31) reads in storage means of a second entity a list of identifiers in complete form of first entities that are smart card proprietors (operation 2), said list being linked to the status assigned to each of the first entities by the second entity, and

[see col. 4, lines 37-43] "In this verification, the reader 2 uses the pieces of digital data representing the identity (contained in the zone 3), the state of the interaction counter (contained in the zone 5) and the state of the balance (contained in the zone 6) to prepare a signature. This signature is entered by the reader applying a DES type algorithm carried out by a DES operator (FIG. 1)."

the chip (31) compares the identifiers stored in the storage means (32) of the chip (31) and the contents of the list (operation 3) to authorize (operation 5) or prohibit (operation 4) calculation by the calculation means (33) as a function of the result of the comparison.

[see col. 4, lines 44-49] "As soon as the reader 2 has prepared this signature, it compares it with the signature already recorded beforehand as a certificate in the card and currently stored in the zone 4 of the card 1. To do this, the reader reads the content of the zone 4 and compares it in its logic comparator with the signature that it has just computed."

As per claim 2, Le Roux teaches:

A cryptographic method according to claim 1, wherein the list comprises all first entities whose status has been set to "revoked" by the second entity and the chip (31) authorizes calculation (operation 5) only if the identifier stored in the storage means (32) of the chip (31) is not in the list.

> *[see col. 5, lines 55-68, col. 6, lines 1-2] "To this end, during the first check, the identity of the card is compared with all the prohibited identities contained in the black list."*

As per claim 3, Le Roux teaches:

A cryptographic method according to claim 1, wherein the list comprises all first entities whose status has been set to "non-revoked" by the second entity and wherein the chip (31) authorizes calculation (operation 5) only if the identifier stored in the storage means (32) of the chip (31) is in the list.

> *[see col. 4, lines 49-51] "If the comparison shows that the two signatures are equal, it is possible to pass on to the purchasing operation itself."*

As per claim 4, Le Roux teaches:

A cryptographic method according to claim 1, further comprising the following steps: at the same time as reading the list (operation 2), the chip (31) reads a signature in the list in the storage means of the second entity (operation 10), which signature was calculated beforehand by calculation means of the second entity, and before the chip (31) authorizes calculation by the calculation means (33) (operation 5), it verifies the validity of the signature (operation 11).

> *[see col. 4, lines 44-49] "As soon as the reader 2 has prepared this signature, it compares it with the signature already recorded beforehand as a certificate in the card and currently stored in the zone 4 of the card 1. To do this, the reader reads the content of the zone 4 and compares it in its logic comparator with the signature that it has just computed."*

As per claim 6, Le Roux teaches:

A smart card (30) for implementing a method according to claim 1, wherein the smart card (30) is equipped with a chip (31) which comprises:

storage means (32) for storing a secret key and an identifier of a first entity that is a proprietor of the smart card,

[see fig. 1, element 1]

calculation means (33) adapted to execute a cryptographic algorithm whose input arguments include the secret key,

> *[see col. 1, lines 27-31] "In this card, the microprocessor fulfils an obvious role of security. In effect, in a card such as this, a microprocessor such as this is capable of applying a complex algorithm for computing or verifying a secret code from a piece of identification data indicated to it."*

reading means (34) for reading from storage means of a second entity via a telecommunications network, a list in complete form of identifiers of first entities that are smart card proprietors, said list being linked to each status assigned to each of the first entities by the second entity, and

> *[see col. 1, lines 31-36] "After this chip card has been introduced into a reader, if the secret code computed is not equivalent to secret code already contained in the card, it becomes impossible to perform an operation with this card, it being known that, in this case, the piece of identification data is false."*

means (35) for comparing the identifier stored in the storage means (32) of the chip (31) and the contents of the list to authorize or prohibit calculation by the calculation means (33) as a function of the result of the comparison.

[see above, "...impossible to perform an operation with this card.."]

CONCLUSION

The art made of record and not relied upon is considered pertinent to applicant's disclosure.

POINTS OF CONTACT

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450

Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel L. Hoang
3/21/07

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/22/07